Chapter 2: Joining the FERMI Domain

In this chapter we discuss placing your computer in the FERMI domain.

2.1 Requirements

In order for your Windows computer to join the FERMI domain, it must run Windows 2000 Desktop/Server, or Windows XP (Professional, not the home edition). A set of security policies and software are required to be deployed on computers that become members. The software installation must be done by whoever supports your machine, e.g., yourself, TOC[1], or a designated person in your group. Domain computers must run:

- anti-virus software (once installed, it automatically obtains updated signature files as needed)
- current required Operating System Patches (see `http://pseekits.fnal.gov/fermi-rollup`)

Only OU managers have the authority to add machines to the FERMI domain. If you determine that your machine should be added, you or your supervisor should arrange it with your OU manager.

2.2 Kerberos Principals and Primary Accounts

You will need to obtain a Kerberos principal if you don't already have one. Your Kerberos principal for the FERMI domain is your account. Request this (and other items as necessary) using the *Request Form for Computing Username and Primary Accounts* at `http://www.fnal.gov/cd/forms/acctreq_form.html`.

[1] A representative of the CD/CSS/TOC group (if your organization maintains an MOU with them).

Note that once you have a FERMI domain principal and password, you also have a principal and password for the FNAL.GOV realm. This realm is for UNIX machines. Connecting to remote UNIX hosts from your W2K desktop is discussed in section Chapter 6: *Networking Beyond the FERMI Windows 2000 Domain*.

2.3 Kerberos Passwords

As a member of the FERMI W2K domain, your OU administrator must enable your FERMI domain account and issue you an initial Kerberos password. You are requested to change this password the first time you log into the domain. Choose a unique password with the following characteristics:

- Does not contain your name or username.
- Contains at least ten characters.
- Contains characters from each of the following three groups:
  - Uppercase and/or lowercase letters
  - Numerals (0 through 9)
  - Symbols (characters that are not defined as letters or numerals, such as !, @, #, and so on)
- Is very hard for a person or program to guess

Please treat your Kerberos password as a sacred object, and adhere to the following rules:

- Your Kerberos password must be known only to you.
- Make sure that you do not write it down anywhere that someone could find it.
- Do not put it in a file (encrypted or not).
- As a usual practice, type it only at the console of a system on which you authenticate.
- Only on very rare occasions, when you have no other choice, may you pass it over a network connection. The connection MUST BE ENCRYPTED. Verify that ALL connections in the chain are encrypted.
- Choose a character string different from your Kerberos password for all other passwords and other objects. (The one exception: your passwords for the FNAL.GOV and FERMI.WIN.FNAL.GOV realms can be the same.)
- If you mistakenly type your Kerberos password over the network on an unencrypted channel, please change your password immediately!

See section 3.5 *Changing your Kerberos or Local Password* for instructions on changing your Kerberos (FERMI domain) password.

If you plan to do connect over the network to remote UNIX hosts, you must change your password in the FNAL.GOV domain within 30 days of issuance; instructions can be found at `http://www.fnal.gov/docs/strongauth/html/princ_pw.html#46115` in the *Strong Authentication at Fermilab* manual for information.

2.4 Off-site Use

For security reasons, a NetBIOS block is in place which blocks access to the FERMI domain controllers. You can still access domain servers from off-site if you have cached Kerberos credentials. How does this work? Log into the FERMI domain and authenticate when you're on-site. Your system will cache a set of credentials automatically. When you take the machine off-site, again log into the FERMI domain (see section 3.2 *Logging In*). In other words, always log into the domain, never into the desktop. Your cached credentials will allow you to communicate with individual file servers, but you will need to map each drive manually (see section 3.11.7 *Mapping Network Drives*).

For more information, see **Sitewide NetBIOS Block**.